ELSEVIER

Journal of Pure and Applied Algebra 144 (1999) 213–227

JOURNAL OF PURE AND APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

Free polynomial generators for the Hopf algebra QSym of quasisymmetric functions

E.J. Ditters [a,*], A.C.J. Scholtens [b]

[a] *Vrije Universiteit, Faculteit der Wiskunde en Informatica, De Boelelaan 1081, 1081 HV Amsterdam, Netherlands*

[b] *Charles Crammweg 2, 6871 HZ Renkum, Netherlands*

Communicated by C. Kassel; received 1 September 1997; received in revised form 11 February 1998

Abstract

In the proof of [11, Corollary 2], of Malvenuto and Reutenauer showed that the set of Lyndon words $\mathscr{L}$ in the language over the alphabet of positive integers is a set of free polynomial generators for the ring $\mathsf{QSym}_{\mathbb{Q}}$ of quasisymmetric functions over the field $\mathbb{Q}$ of rational numbers. A slight modification of the definition of Lyndon words permits to present a set of free polynomial generators for the ring QSym of quasisymmetric functions over the ring of rational integers $\mathbb{Z}$.

MSC: Primary 16W30; secondary 05E99; 08A50

1. Introduction

We let $\mathscr{Z}$ be the free noncommutative associative algebra generated over $\mathbb{Z}$ by a denumerable set of noncommuting quantities $\{z_i \mid i \geq 1\}$. For convenience put $z_0 := 1$. The sextuple $(\mathscr{Z}, \Delta, \varepsilon, \mu, \eta, S)$ is a Hopf algebra, fully determined by the following conditions: as an algebra $(\mathscr{Z}, \mu, \eta)$ has the structure of a free noncommutative polynomial ring over $\mathbb{Z}$; viewed as a coalgebra $(\mathscr{Z}, \Delta, \varepsilon)$, the set $\{z_n \mid n \geq 0\}$ is a sequence of divided powers in $\mathscr{Z}$ lying over 1, equivalently

$$\Delta(z_n) = \sum_{a+b=n} z_a \otimes z_b \quad \text{for } n \geq 0. \tag{1}$$

* Corresponding author. Fax: 0031 20 4448054; e-mail: ejd@cs.vu.nl.

0022-4049/99/$ - see front matter
PII: S0022-4049(98)00066-8

An easy computation shows that if $\{u_n \mid n \geq 0\}$ and $\{v_n \mid n \geq 0\}$ are two sequences of divided powers lying over 1, then the sequence $\{w_n \mid n \geq 0\}$, where

$$w_n = \sum_{a+b=n} u_a v_b \quad \text{for } n \geq 0 \tag{2}$$

is a sequence of the divided powers lying over 1. In fact these sequences constitute a group. The neutral element is the constant sequence $\{v_n \mid n \geq 0\}$ where $v_0 = 1$ and $v_n = 0$ for $n > 0$. The inverse $u^{-1}(= v)$ of the sequence u can be computed by solving recurrently v_b from (2) with $w_n = \delta_{n,0}$, the Kronecker delta. See [2] for a discussion of these sequences, called *curves*, in the setting of Cartier duality for formal (co)groups. We refer to loc. cit. for the definition of the finite sequences of the divided powers. If Hopf_K is the category of Hopf algebras over the commutative unitary base ring K and $\mathsf{SDP}(H)$ is the group of sequences of divided powers in H, then $\mathscr{Z}_K := K \otimes \mathscr{Z}$ represents $\mathsf{SDP}(H)$ for $H \in \mathsf{Hopf}_K$ via the functorial bijection

$$\mathsf{Hopf}_K(\mathscr{Z}_K, H) \cong \mathsf{SDP}(H). \tag{3}$$

Here the Hopf algebra morphism $f: \mathscr{Z}_K \to H$ corresponds to the sequence $\{f(z_n) \mid n \geq 0\}$. Therefore, a morphism of unitary rings $f: \mathscr{Z}_K \to H$, commuting with the structural (co)augmentation and antipodism is a morphism of Hopf algebras if and only if $f \otimes f \circ \Delta = \Delta \circ f$. Applying this relation to (1), we at once see that

$$f \otimes f \circ \Delta(z_n) = \sum_{a+b=n} f(z_a) \otimes f(z_b) = \Delta(f(z_n)),$$

where the second "=" displays the fact that $\{f(z_n) \mid n \geq 0\}$ in this way becomes a sequence of the divided powers in H. Since the morphism f of an unitary rings is determined completely by the images $f(z_n)$, $n \geq 1$, formula (3) follows. We will write a sequence $\{x_n \mid n \geq 0\}$, $x_0 = 1$ in the form $x = \sum_{n=0}^{\infty} x_n t^n$ or $\sum_n x_n t^n$, identifying it with its image in the multiplicative group $1 + tH[[t]]$. In fact we have:

Lemma 1.1. *The map* $\lambda : \mathsf{SDP}(H)1 + tH[[t]]$, *given by*

$$\lambda(\{x_n \mid n \geq 0\}) := \sum_{n=0}^{\infty} x_n t^n$$

is a homomorphism of groups, where the group structure on the target is given by multiplication of the formal powerseries in t with (*not necessarily commuting*) *coefficients in H.*

Proof. Ditters [2, Lemma 1.2]. □

$\mathsf{SDP}(H)$ admits the following two operators: the ath-Verschiebung V_a ($a > 0$ in $\mathbb{Z}$), defined by $t \mapsto t^a$ and for every α in the base ring the homothety $[\alpha]$, defined by $t \mapsto \alpha t$.

In terms of the power series one has

$$V_a\left(\sum_n x_n t^n\right) = \sum_n x_n t^{an}$$

and

$$[\alpha]\left(\sum_n x_n t^n\right) = \sum_n (\alpha^n x_n t^n).$$

The sequences of divided powers play a fundamental role in the classification of formal groups (formal group laws).

A second appearance exhibits $\mathscr{Z}$ as the generic ring of noncommutative symmetric functions, see [5]. But in this note we have no applications for this fact.

For the third context where $\mathscr{Z}$ plays a central role we first recall some definitions. A *composition* or *word* w of *length* $\lambda(w)=k$ and *weight* $|w|=n$ is a sequence $w=(w_1,\ldots,w_k)$ of positive integers with $|w|:=\sum_{i=1}^{k} w_i = n$. Equivalently, if $\mathbb{N}_+$ is the set of positive integers, then w is a word of length k in the language $\mathbb{N}_+^\star$ over the alphabet $\mathbb{N}_+$ and the sum of its digits equals n. The empty sequence is called the empty word, denoted by 1. The set of all compositions or words is denoted by Comp. The natural order on $\mathbb{N}_+$ induces the total lexicographical order on $\mathbb{N}_+^\star$. Since $\mathbb{N}_+^\star$ is an associative monoid under concatenation, one can speak about factorizations of words. A word w is called a *Lyndon word*, denoted by $w\in\mathscr{L}$, if for every non trivial factorization $w=xy$ in $\mathbb{N}_+^\star$ one has $y>w$. Of course, we could have taken as a point of departure the set $\mathbb{N}$ of all nonnegative integers as well and speak about *pseudo-compositions* or *pseudowords*. Recall that the ring QSym of quasisymmetric functions is defined as follows (see [11, Section 9.4]): Let X be a totally ordered alphabet and let $\mathbb{Z}[[X]]$ be the ring of the formal power series over $\mathbb{Z}$ generated by the elements of X. $F\in\mathbb{Z}[[X]]$ of finite degree is called *quasisymmetric*, if, firstly, for every choice of $k\geq 0$ in $\mathbb{N}$, secondly, for every choice of $x_1<\cdots<x_k$ and $y_1<\cdots<y_k$ in X and finally, if for every composition $w=(w_1,\ldots,w_k)$ the coefficients of the monomials $x_1^{w_1}\cdots x_k^{w_k}$ and $y_1^{w_1}\cdots y_k^{w_k}$ are the same. Replacing the second condition by arbitrary choices of $x_1,\ldots,x_k$ and $y_1,\ldots,y_k$, we refind the well-known ring Sym of symmetric functions. Define for every composition w the monomial quasisymmetric function M_w by

$$M_w := \sum_{x_1<\cdots<x_k} x_1^{w_1}\cdots x_k^{w_k} \tag{4}$$

and let $\{M_w^\star \mid w\in\mathsf{Comp}\}$ be the dual $\mathbb{Z}$-linear basis for $\mathsf{QSym}^\star$. We often identify M_w in (4) with the composition w. As customary, if $\{X_w \mid w\in\mathsf{Comp}\}$ is a set of quantities indexed by the compositions, we write X_m instead of $X_{(m)}$. Equally, if $w=(w_1,\ldots,w_k)\in\mathsf{Comp}$, we write $z_w:=z_{w_1}\cdots z_{w_k}$. Define $P_m^\star$ $(m\geq 0)$ in $(\mathsf{QSym}^\star)_{\mathbb{Q}}$

by the condition

$$\sum_{n\geq 0} M_n^\star t^n = \exp\left(\sum_{m=1}^{\infty} P_m^\star t^m\right). \tag{5}$$

Notice the following fact in the context of formula (5): let H be a Hopf algebra over $\mathbb{Q}$ and suppose we have in $1+H[[t]]$ the relation

$$\sum_{n\geq 0} x_n t^n = \exp\left(\sum_{m=1}^{\infty} X_m \frac{t^m}{m}\right). \tag{6}$$

Then $\{x_n \mid n\geq 0, x_0 = 1\}$ is a sequence of the divided powers in H if and only if the set $\{X_m \mid m \geq 1\}$ is a set of primitive elements. The scalar factor m^{-1} is added, since this guarantees better integrality properties in the case of the commutative Hopf algebras. For example, one has in that case for every $m \in \mathbb{N}_+$ the fact that $X_m \in \mathbb{Z}[x_n \mid n \geq 1]$, thus X_m is a polynomial in these x_n with integral coefficients.

Malvenuto and Reutenauer proved the following two theorems [8, Theorem 2.1, Corollary 2.3, Eqs. (2.7) and (2.8)]:

Theorem 1.2. $\mathsf{QSym}^\star$ *is an associative noncommutative algebra, freely generated by the elements* $M_n^\star$ *for* $n \geq 1$. $\mathsf{QSym}^\star$ *is a Hopf algebra, where the comultiplication is determined by the fact that* $\{M_n^\star \mid n \geq 0\}$ *is a sequence of the divided powers. Moreover, extending scalars to* $\mathbb{Q}$, *the dual* $\mathsf{QSym}_{\mathbb{Q}}^\star$ *of* $\mathsf{QSym}_{\mathbb{Q}}$ *is the noncommutative associative polynomial ring* $\mathbb{Q}\langle P_m^\star \mid m \geq 1\rangle$, *freely generated over* $\mathbb{Q}$ *by the noncommuting primitive elements* $P_m^\star$ $(m \geq 1)$.

Notice that this theorem permits (via $z_n \mapsto M_n^\star$) the identification of the Hopf algebras $\mathscr{Z}$ and $\mathsf{QSym}^\star$. In order to formulate the second theorem we need a few definitions. Let A be any set and K an integral domain. We denote $K[A]$ as the free commutative polynomial ring generated over K by the elements of A. In particular the elements of A are algebraically independent over the field of the quotients of K. In the notation of [11] it is clear that $K[A]$ is the largest commutative quotient $K\langle A\rangle/J$ of $K\langle A\rangle$ with respect to the two-sided ideal generated by all commutators $[a,b] = ab - ba$ with $a, b \in A$. In the second theorem we identify a Lyndon word w over the positive integers $\mathbb{N}_+$ with the monomial quasisymmetric function M_w of (4). Malvenuto and Reutenauer now prove [8, Corollary 2.2]

Theorem 1.3. $\mathsf{QSym}_{\mathbb{Q}} = \mathbb{Q}[\mathscr{L}]$, *the free commutative polynomial ring generated over* $\mathbb{Q}$ *by the algebraically independent set of Lyndon words.*

Let $a, b \in \mathsf{Comp}$. Define recurrently the *variable length shuffle product* $a \uplus b \in \mathsf{QSym}$ as follows:

- $1 \uplus a = a \uplus 1 = a$,
- writing for every word w of length $\lambda(w) \geq 1$: $w = w_1\hat{w}$ and denoting (for clarity) in the following formula the concatenation uv of the words u and v as $u \star v$ and the

addition on $\mathbb{Z}\langle\mathbb{N}_+\rangle$ the free $\mathbb{Z}$-module on the words over the alphabet of positive integers $\mathbb{N}_+$ by $\oplus$:

$$a \uplus b = (a_1 + b_1) \star (\hat{a} \uplus \hat{b}) \oplus a_1 \star (\hat{a} \uplus b) \oplus b_1 \star (a \uplus \hat{b}). \tag{7}$$

Here, $a_1 + b_1$ is just the sum in $\mathbb{N}_+$ of the two positive integers a_1 and b_1 and the definition determines recurrently the operation $\uplus$, since every $\uplus$-product in the right side is made from words having length $< \lambda(a) + \lambda(b)$.

If $a \uplus b = \sum_w \lambda_{a,b,w} w$ in QSym, then the structure of commutative unitary ring "$\cdot$" on QSym is given by

$$M_a \cdot M_b = \sum_w \lambda_{a,b,w} M_w. \tag{8}$$

Therefore, by (4) we have for $a = (a_1 \cdots a_k)$ and $b = (b_1 \cdots b_m)$,

$$M_a \cdot M_b = \left(\sum_{u_1 < \cdots < u_k} u_1^{a_1} \cdots u_k^{a_k} \right) \cdot \left(\sum_{v_1 < \cdots < v_m} v_1^{b_1} \cdots v_m^{b_m} \right) = \sum_{u_1 = v_1} + \sum_{u_1 < v_1} + \sum_{u_1 > v_1},$$

where the right side is an obvious decomposition of the product in the middle into three separate summations arising from the three possible situations $u_1 = v_1, u_1 < v_1$ and $u_1 > v_1$. But this is the situation expressed by (7). Note that the same operation in different notation appears in [6, Axioms B1 and B2, p. 484].

It is easy to interprete this product in terms of pseudocompositions as follows: let k be any integer such that $\max\{\lambda(a), \lambda(b)\} \leq k \leq \lambda(a) + \lambda(b)$ and let $S_k(a)$ be the set of all shuffles of the word a and the zero pseudocomposition $(0, \ldots, 0)$ of length $k - \lambda(a)$. In the same way let $S_k(b)$ be the set of all shuffles of the word b and the zero pseudocomposition $(0, \ldots, 0)$ of length $k - \lambda(b)$. For $\alpha \in S_k(a)$ and $\beta \in S_k(b)$ we write the word $\alpha + \beta$, obtained by coordinatewise addition in $\mathbb{N}$ as $\alpha \oplus \beta$ if and only if $\alpha + \beta$ is a composition, i.e. if and only if it has no zero digits. Then

$$a \uplus b = \sum_{\substack{k \\ \alpha \in S_k(a), \beta \in S_k(b)}} \alpha \oplus \beta. \tag{9}$$

Examples 1.4.

- $(1) \uplus (2) = (3) + (1,2) + (2,1)$.
- $(1,1) \uplus (2) = (1,3) + (3,1) + (1,1,2) + (1,2,1) + (2,1,1)$.
- $(1)^{\uplus 3} = (3) + 3(1,2) + 3(2,1) + 6(1,1,1)$.

Returning to (5), the expansion over the base ring $\mathbb{Q}$ gives

$$M_1^\star = P_1^\star \quad \text{and} \quad M_n^\star = P_n^\star + Q_n(P_1^\star, \ldots, P_{n-1}^\star) \quad \text{for } n \geq 2, \tag{10}$$

where Q_n is homogeneous of weight n, if one attaches to each $P_n^\star$ the weight n. By Theorem 1.2 or directly from (10) we have $\mathscr{Z}_\mathbb{Q} = \mathbb{Q}\langle P_n^\star \mid n \geq 1 \rangle$ and in view of what has been said about (6) the $P_n^\star$ are primitive. We may write $P_{w_1}^\star P_{w_2}^\star \cdots P_{w_k}^\star$ as $P_w^\star$

where $w=(w_1,\ldots,w_k)$ and consider the $\mathbb{Q}$-vector space basis $\{P^\star_w \mid w\in \mathsf{Comp}\}$. Let $\{P_u \mid u\in \mathsf{Comp}\}$ be the dual basis for $\mathsf{QSym}_{\mathbb{Q}}$. Since all $P^\star_n$ are primitive, it follows that the multiplication on QSym obtained by graded duality, identifying P_u with the composition u, coincides with the usual shuffle product $\sqcup$, see [11, Section 1.4] for details. We may, however, express every element of $\mathscr{Z}^\star$, identified with QSym as well as a $\mathbb{Z}$-linear combination of elements of the basis of monomial quasisymmetric functions $\{M_w \mid w\in \mathsf{Comp}\}\subset \mathsf{QSym}$ dual to $\{z_w \mid w\in \mathsf{Comp}\}\subset \mathscr{Z}$. In this situation, M_u is to be identified with the composition u. If we then consider the multiplication obtained by graded duality, it is not too difficult to see that now the multiplication is expressed by the variable length shuffle product. Indeed, if we denote

$$\langle ?,?\rangle : \mathscr{Z}\times \mathsf{QSym}\to\mathbb{Z}$$

the canonical evaluation map obtained from the identification of $\mathscr{Z}$ with $\mathsf{QSym}^\star$, we have for variable $w=(w_1,\ldots,w_n)$,

$$\begin{aligned}\langle z_w, \Delta^\star(a\otimes b)\rangle &= \langle \Delta(z_w), a\otimes b\rangle\\ &= \left\langle \sum_{u_1+v_1=w_1,\ldots,u_n+v_n=w_n} z_{u_1\cdots u_n}\otimes z_{v_1\cdots v_n}, a\otimes b\right\rangle. \end{aligned}\tag{11}$$

It should be noted that $u=(u_1\cdots u_n)$ and $v=(v_1\cdots v_n)$ are pseudocompositions, since $z_0=1$ intervenes in every $\Delta(z_n)$, see (1). Further, if $\Delta^\star(a\otimes b)=\sum_w c_w w$, then c_w is the coefficient of $a\otimes b$ in $\Delta(z_w)$. Consider a typical term in the right side of (11). In order to give a nonzero contribution, there are only three possibilities for the pair (u_1,v_1) namely $(u_1,v_1)=(a_1,b_1),(a_1,0)$ and $(0,b_1)$. Suppose we have for every word w and for every x and y with $\lambda(x)+\lambda(y)<\lambda(a)+\lambda(b)$:

$$\langle z_w,\Delta^\star(x\otimes y)\rangle = \left\langle \sum_{u_1+v_1=w_1,\ldots,u_n+v_n=w_n} z_{u_1\cdots u_n}\otimes z_{v_1\cdots v_n}, x\otimes y\right\rangle = \langle z_w, x\uplus y\rangle. \tag{12}$$

On the basis of this assumption we evaluate the sum of the three possibilities in (11), according to (12) and using the notation of (7) as

$$a\uplus b=(a_1+b_1)\star(\hat{a}\uplus\hat{b})\oplus a_1\star(\hat{a}\uplus b)\oplus b_1\star(a\uplus\hat{b}),$$

which is indeed formula (7). Note that the variable length shuffle product is the result of basis transformation (10) from the set of primitive generators $\{P^\star_m \mid m\geq 1\}$ for $\mathsf{QSym}^\star_{\mathbb{Q}}=\mathscr{Z}_{\mathbb{Q}}$ to the generating set $\{M^\star_n=z_n \mid n\geq 1\}$ for $\mathscr{Z}\subset\mathscr{Z}_{\mathbb{Q}}$, constituting together with 1 the generic sequence of the divided powers.

If $w=(w_1,\ldots,w_k)\in\mathsf{Comp}$ is a nonempty word, we let $\gcd(w)$ be the greatest common divisor of all digits w_i. Put $w_{\mathrm{red}}:=(w_1/\gcd(w),\ldots,w_k/\gcd(w))$. Define for Lyndon words in $\mathbb{N}^\star_+$ the map

$$\phi:\mathscr{L}\to\mathsf{Comp},\tag{13}$$

by

$$\phi(w) := w_{\mathrm{red}}^{\gcd(w)},$$

where the power is to be interpreted in the concatenation structure. The image $\mathrm{Im}(\phi)$ will be denoted by $\mathscr{L}^{\mathrm{mod}}$ and its elements are called *modified Lyndon words*. Note ϕ is weight preserving and injective.

Observe that $\phi(w)$ is a Lyndon word itself if and only if $\gcd(w) = 1$ and in that case we have $\phi(w) = w$. In the next theorem, the main theorem of this study, we identify as usual the quasisymmetric function M_w of (4) with the composition w.

Theorem 1.5 (Main theorem)**.** *As a commutative algebra,* $(\mathsf{QSym}, \uplus)$ *is equal to* $\mathbb{Z}[\mathscr{L}^{\mathrm{mod}}]$, *the free commutative polynomial ring generated over* $\mathbb{Z}$ *by the the algebraically independent set of modified Lyndon words. Here the presence of the symbol* $\uplus$ *expresses the fact that every nonempty word w can be expressed as a* (*unique*) $\mathbb{Z}$*-linear combination of elements of the set* $\{m_1 \uplus \cdots \uplus m_k \mid k > 0, m_1 \leq m_2 \leq \cdots \leq m_k, m_i \in \mathscr{L}^{\mathrm{mod}}\}$, *thus as a unique* $\mathbb{Z}$*-linear combination of* $\uplus$*-products of modified Lyndon words.*

Postponing the proof of the main theorem to Section 3 we note the following corollary.

Corollary 1.6. (a) *The subalgebra of the symmetric functions* Sym *is freely generated over* $\mathbb{Z}$ *by the set of words* $\{\phi((n)) = (1,\ldots,1) = (1)^n =: \varepsilon_n \mid n \geq 1\}$.

(b) QSym *is a free module over* Sym.

Proof. Part (a) is well known, see [7], but it is also a direct consequence of the main theorem. Also part (b) is equally obvious from the main theorem, if one observes that $\{\varepsilon_n \mid n \geq 1\} = \mathscr{L}^{\mathrm{mod}} \cap \mathsf{Sym}$. It strengthens the corresponding result over $\mathbb{Q}$, see [8, Corollary 2.2], of Malvenuto and Reutenauer to the case that the base ring is $\mathbb{Z}$. □

The main theorem appears in [3, Theorem 4.5], unpublished, together with an outline of the proof, see also [12]. The theorem on unique descending factorization of Hall words, together with the fact that the set of Lyndon words is a Hall set in view of [11, Corollary 4.7 and Theorem 5.1] permitted essential simplifications of the proofs, as given in [3, 12].

2. Some other corollaries

The main theorem permits a complete description, at least in principle, of the $\mathbb{Z}$-Lie algebra of primitives

$$\mathscr{P}(\mathscr{Z}) = \{z \in \mathscr{Z} \mid \Delta(z) = z \otimes 1 + 1 \otimes z\}.$$

By Theorem 1.2 we know that $\mathscr{P}(\mathscr{Z}_{\mathbb{Q}})$ is a free Lie algebra over the set $\{P_n^\star \mid n \geq 1\}$, but we have

Lemma 2.1. *$\mathscr{P}(\mathscr{Z})$ is not a free Lie algebra over $\mathbb{Z}$ in the sense of* [11, *Section* 0.2].

Proof. Suppose $\mathscr{P}(\mathscr{Z})$ is a free Lie algebra on the set A. We then may take a total order $<$ on A. Consider the $\mathbb{Z}$-module basis $\{1, z_1, 2z_2 - z_1^2, z_2\}$ for the space H_2 of homogeneous elements of weight ≤ 2 in $\mathscr{Z}$. Since z_1 and $2z_2 - z_1^2$ constitute a $\mathbb{Z}$-module basis for the primitives $\mathscr{P}(\mathscr{Z}) \cap H_2$, they correspond to elements a, b in the set A. Take a Hall set H in the free magma $M(A)$ of A, existing in view of [11, Theorem 4.1].

In view of [11, Theorem 4.9, Example 4.8] one concludes that the three Hall polynomials a, b and $[a, b] = ab - ba$ are part of a $\mathbb{Z}$-module basis of $\mathscr{P}(\mathscr{Z})$. In particular, the $\mathbb{Z}$-module $T := \mathscr{P}(\mathscr{Z})/(\mathbb{Z}a + \mathbb{Z}b + \mathbb{Z}[a, b])$ should be a free $\mathbb{Z}$-module. But computation shows that $[a, b] = 2[z_1, z_2]$ is primitive. Since $[z_1, z_2]$ does not belong to $\mathbb{Z}a + \mathbb{Z}b + \mathbb{Z}[a, b]$, but $2[z_1, z_2]$ does, we see that T has 2-torsion and thus it is not a free $\mathbb{Z}$-module. It follows that $\mathscr{P}(\mathscr{Z})$ is not free on the set A. □

Let $\varepsilon: \mathsf{QSym} \to \mathbb{Z}$ be the canonical augmentation on QSym sending every nonempty word w to 0 and put $J := \mathrm{Ker}(\varepsilon)$. Let $\mathsf{QSym}\hat{}$ be the completion of QSym with respect to the J-adic topology. Consider a continuous homomorphism of the $\mathbb{Z}$-algebras $\phi: \mathsf{QSym}\hat{} \to \mathbb{Z}[[t]]$. Here $\mathbb{Z}$ is equipped with the discrete topology. We may write as in [2, Section 1.5]

$$\phi(x) = \sum_{i=0}^{\infty} \phi_i(x) t^i \quad \text{for } x \in \mathsf{QSym} \tag{14}$$

and deduce as in loc. cit. that all $\phi_i \in \mathscr{Z}$. We obtain in this way a bijection between the set of sequences of divided powers $\{\phi_i \mid i \geq 0\} \in \mathsf{SDP}(\mathscr{Z})$ and the set of continuous unitary ring homomorphisms $\{\phi : \mathsf{QSym}\, \mathbb{Z}[[t]]\}$. In particular, define the unitary ring homomorphisms ϕ_u for $u \in \mathscr{L}^{\mathrm{mod}}$ by

$$\phi_u(v) := \delta_{u,v} t \quad \text{for } v \in \mathscr{L}^{\mathrm{mod}}.$$

Writing as in Lemma 1.1

$$\phi_u = \sum_{i=0}^{\infty} \phi_{u,i} t^i, \tag{15}$$

we then have the following result

Corollary 2.2. (a) *The set $\{\phi_{u,1} \mid u \in \mathscr{L}^{\mathrm{mod}}\}$ is a $\mathbb{Z}$-module basis for the Lie algebra of primitives in $\mathscr{Z}$.*

(b) *Such an element $\phi_{u,1}$ of this basis is completely characterized by the conditions of being primitive and having zero coefficient in z_w for every $w \in \mathscr{L}^{\mathrm{mod}}$ with $w \neq u$.*

Proof. By (graded) duality the primitives in the graded Hopf algebra $\mathscr{Z}$ over $\mathbb{Z}$ correspond bijectively to the $\mathbb{Z}$-module of linear maps $f: \mathsf{QSym} = \mathbb{Z}[\mathscr{L}^{\mathrm{mod}}] \to \mathbb{Z}$ that are zero on the constants and on the elements that belong to the ideal J^2. This implies that for $v_i \in \mathscr{L}^{\mathrm{mod}}$,

$$\phi_{u,1}(v_1 \cdots v_k) = 0 \quad \text{if } k > 1,$$

and for modified Lyndon words u and v,

$$\phi_{u,1}(v) = \delta_{u,v}. \tag{16}$$

Part (a) now results from the bijection $(J/J^2)^\star \cong \mathscr{P}(\mathscr{Z})$. Part (b) is a direct consequence of (16). □

Let $\mathsf{M}(\mathbb{N})$ be the set of all multi-indices over $\mathbb{N}$. Thus $\alpha \in \mathsf{M}(\mathbb{N})$ if and only if $\alpha = (\alpha_i \mid \alpha_i = 0$ for almost all $i)$. Observe that we may write $\alpha \in \mathsf{M}(\mathbb{N})$ in the finite form $\alpha = (\alpha_1, \ldots, \alpha_r)$ for some $r \geq 1$. The set $\mathsf{M}(\mathbb{N})$ is an abelian monoid under componentwise addition. Define in the context of (15) for every multi-index $\alpha = (\alpha_1, \ldots, \alpha_r) \in \mathsf{M}(\mathbb{N})$ and $u_1 < u_2 < \cdots < u_r$ in $\mathscr{L}^{\mathrm{mod}}$ the element $\phi_\alpha \in \mathscr{Z}$ by $\phi_\alpha := \phi_{u_1,\alpha_1} \cdots \phi_{u_r,\alpha_r}$. The following fact is a straightforward verification:

Corollary 2.3. *The set* $\{\phi_\alpha \mid \alpha \in \mathsf{M}(\mathbb{N})\}$ *is a structural basis for* $\mathscr{Z}$ *in the sense of Dieudonné. This means in particular that*

$$\Delta(\phi_\alpha) = \sum_{\beta+\gamma=\alpha} \phi_\beta \otimes \phi_\gamma, \quad \alpha \in \mathsf{M}(\mathbb{N}).$$

Proof. By standard dualization techniques as in [1]. □

The following corollary treats the problem of extension of sequences of divided powers in a Hopf algebra H. Given two finite sequences of divided powers $x = \{x_n \mid 0 \leq n \leq M\}$ and $y = \{y_n \mid 0 \leq n \leq N\}$ in H, we say that the sequence y extends the sequence x, if $N \geq M$ and $x_n = y_n$ for $0 \leq n \leq M$. While extension of such sequences is always possible over the base field $\mathbb{Q}$ – which in fact is an easy consequence of (6) – it is in general not possible over other base rings. Consider for example the Hopf algebra $H = \mathbb{Z}[x]$ where x a primitive element, thus $\Delta(x) = x \otimes 1 + 1 \otimes x$ and $x \mapsto -x$ under the antipode of H. It can be computed directly, or seen from [9, Theorem 1 or Table 1], that there is no extension $y = \{1, x, u\}$ of $x = \{1, x\}$. Over $\mathbb{Q}$ we could take the extension $\{\frac{x^n}{n!} \mid n \geq 0\}$.

Corollary 2.4. *Every finite sequence of the divided powers in* $\mathscr{Z}$ *can be extended to an infinite sequence.*

Proof. The proof relies heavily on Lemma 1.1 and we use this lemma without further explicit reference. Let $\xi = \sum_{i=0}^{N} \xi_i t^i$ be such a finite sequence. If $N = 0$, then there is nothing to prove, since the trivial series $\xi = 1 = 1 + \sum_{i=1}^{\infty} \xi_i$ with $\xi_i = 0$ for $i \geq 1$ is an

infinite sequence of the divided powers. Thus let $N=1$. Then ξ_1 is primitive, hence by Corollary 2.2(a) we have

$$\xi_1=\sum_u \lambda_{u,1}\phi_{u,1},$$

a finite $\mathbb{Z}$-linear combination of basis primitives. It follows that

$$\xi\equiv\prod_u [\lambda_{u,1}]\phi_u \bmod t^2.$$

The right side is to be considered as an *ordered* product of infinite sequences of divided powers, say for the lexicographic order on $\mathscr{L}^{\mathrm{mod}}$, hence is itself such an infinite sequence of the divided powers. Thus assume

$$\xi\equiv\prod_{a=1}^{M} V_a\left(\prod_u [\lambda_{u,a}]\phi_u\right)\bmod t^{M+1}, \tag{17}$$

where the right side is an ordered product of infinite sequences of divided powers, say a V_a-product precedes a V_b-product if $a<b$. If $M=N$ we are done. Thus let $M<N$. Write the right side in the form $\sum_{i=0}^{\infty}\chi_i t^i$. Then it is easily verified that the difference $\xi_{M+1}-\chi_{M+1}$ is primitive, hence

$$\xi_{M+1}-\chi_{M+1}=\sum_u \lambda_{u,M+1}\phi_{u,1}$$

is a finite $\mathbb{Z}$-linear combination of basis primitives. It follows that

$$V_{M+1}\prod_u [\lambda_{u,M+1}]\phi_u\equiv 1+(\xi_{M+1}-\chi_{M+1})t^{M+1}\bmod t^{M+2}.$$

Next,

$$\begin{aligned}\xi&\equiv\prod_{a=1}^{M}\left(V_a\prod_u[\lambda_{u,a}]\phi_u\right)\left(V_{M+1}\prod_u[\lambda_{u,M+1}]\phi_u\right)\\&\equiv\prod_{a=1}^{M+1}\left(V_a\prod_u[\lambda_{u,a}]\phi_u\right)\bmod t^{M+2},\end{aligned}$$

which completes in view of (17) the proof by induction. □

3. Proof of the main theorem

The proof will proceed in a number of steps.

Step 1. Let $w\in\mathsf{Comp}$ and consider the descending factorization of w into Lyndon words

$$w=l_1^{e_1}\cdots l_k^{e_k}\quad\text{with } l_1>\cdots>l_k \text{ in } \mathscr{L} \text{ and } \min\{e_1,\ldots,e_k\}\geq 1. \tag{18}$$

Such a factorization exists, e.g. [11, Corollary 4.7 and Theorem 5.1]. Recall an identity [11, Theorem 6.1]

$$\frac{l_1^{\sqcup e_1} \sqcup \cdots \sqcup l_k^{\sqcup e_k}}{e_1! \cdots e_k!} =: \sum_{u<w} \beta_u u + w \quad \text{with } \beta_u \in \mathbb{N}. \tag{19}$$

This identity is the basic identity for the theorem, due to Radford, [10, Theorem 3.1.1e, p. 446], that $\mathsf{QSym}_{\mathbb{Q}}$ is the free polynomial ring, generated over $\mathbb{Q}$ by the Lyndon words. In order to find a relation valid for the base ring $\mathbb{Z}$ we modify (19) and consider instead the expression

$$l_1^{e_1} \uplus \cdots \uplus l_k^{e_k} =: \sum_u \alpha_u u \quad \text{with } \alpha_u \in \mathbb{N}. \tag{20}$$

Here the symbols $l_i^{e_i}$ are e_i-fold concatenation powers of l_i. Moreover, the shuffle products between the $\sqcup$-powers of the various l_i in (19) now are replaced by the variable length shuffle product. Finally, denominators in (20) are not present any more. The basic property of (20) is

Lemma 3.1. *Define the canonical order "$\prec$" on* Comp, *for which $u \prec v$, or equivalently, $v \succ u$, if $\lambda(u) < \lambda(v)$, and if $\lambda(u) = \lambda(v)$, then $u \prec v$ if and only if $u < v$, i.e. the canonical order is determined by the length of the words, and if the lengths are equal, then the lexicographic order determines the canonical order. If* (18) *is the canonical descending factorization of the word w, then*

$$l_1^{e_1} \uplus \cdots \uplus l_k^{e_k} = \sum_{u \prec w} \alpha_u u + w \quad \textit{with } \alpha_u \in \mathbb{N}. \tag{21}$$

Notice that the descending factorization of w is taken in the lexicographic order while the right side of (21) is written in the canonical order.

Proof. Write the right side of (20) in the form $\sum_1 + \sum_2$, where in $\sum_1$ all terms $\alpha_u u$ are collected for which $\alpha_u \neq 0$ and $\lambda(u) < \lambda(w)$. Now observe the following facts:

- No term $\alpha_u u$ in $\sum_1$ with $\alpha_u \neq 0$ occurs as $\beta_u u$ with $\beta_u \neq 0$ in the right side of (19). This results from the facts that $\lambda(u) < \lambda(w)$ and that all words u in (19) have length $\lambda(w)$.
- If a term $\alpha_u u$ occurs in $\sum_2$, then u occurs in (19) with the same coefficient. Indeed, if $\alpha_u u$ occurs in $\sum_2$, then it has length $\lambda(w)$, hence u is an ordinary shuffle of the k words $l_i^{e_i}$. Since all $l_i^{e_i}$ are different, we even have $\alpha_u = 1$. Now u may be considered too as a shuffle of the $\sum_i e_i$ words $l_1, \ldots, l_1, l_2, \ldots, l_2, \ldots, l_k, \ldots, l_k$, where each l_i has multiplicity e_i. There are $e_1! \cdots e_k!$ possibilities for the realization of u as a shuffle of these $\sum_i e_i$ words. Since the left side of (19) must be divided by this product, we see that $\alpha_u u$ occurs in (19) with coefficient $\beta_u = 1$.
- As proven in [11, Theorem 6.1], w is the maximal lexicographic term in (19) with coefficient 1. Since we saw that every word of length $\lambda(w)$ in $\sum_2$ occurs in (19), and since in particular this applies for the word w itself, we see that w must be

the maximal lexicographical word in $\sum_2$, thus w is the maximal canonical word in (21). □

From the lemma we immediately deduce by triangularity:

Corollary 3.2. *The set*

$$\mathscr{B} = \{l_1^{e_1} \uplus \cdots \uplus l_k^{e_k} \mid l_1 > \cdots > l_k \text{ in } \mathscr{L}, k \geq 0\} \tag{22}$$

is a $\mathbb{Z}$-module basis for QSym.

Incidentally, we have the following result that will be used in the next step:

Corollary 3.3. *For $u \in$ Comp we let $\mathscr{L}(u)$ be the set of Lyndon words l that are lexicographically smaller than or equal to u. Let $w \in$ Comp and $l \in \mathscr{L}$ be words with $w < l$. Write w as an element of $\mathbb{Q}[\mathscr{L}]$. Then w belongs to the subring $\mathbb{Q}[\mathscr{L}(w)]$, that is, l does not occur in the expression of w written as a polynomial in Lyndon words.*

Proof. Obvious from triangularity. □

Step 2. The second step will be stated as a lemma.

Lemma 3.4. $(\mathsf{QSym}_{\mathbb{Q}}, \uplus) = \mathbb{Q}[\mathscr{L}] = \mathbb{Q}[\mathscr{L}^{\mathrm{mod}}]$ *and the set $\mathscr{L}^{\mathrm{mod}}$ is algebraically independent.*

According to the definition of $\mathbb{Q}[A]$ for a set A as given before and the meaning of the notation $(\mathsf{QSym}_{\mathbb{Q}}, \uplus)$ as in the main theorem, but now considered over the base ring $\mathbb{Q}$, the statement of the lemma implies that within the algebra $\mathsf{QSym}_{\mathbb{Q}}$, identified by Theorem 1.3 with $\mathbb{Q}[\mathscr{L}]$, we can take instead of $\mathscr{L}$ the elements of $\mathscr{L}^{\mathrm{mod}}$ as algebraically independent polynomial generators.

Proof. By [11, Theorem 6.1] and the identification $\mathbb{Q}[\mathscr{L}]$ and $\mathsf{QSym}_{\mathbb{Q}}$, the ring generated over $\mathbb{Q}$ by the modified Lyndon words is contained in $\mathbb{Q}[\mathscr{L}]$. We shall show the converse inclusion. Let $l \in \mathscr{L} \setminus \mathscr{L}^{\mathrm{mod}}$, then $\gcd(l) > 1$. We claim that for every word w with $(a :=) \gcd(w) > 1$ we have

$$(w_{\mathrm{red}})^{\uplus a} = \sum_{u < w} a_u u + w \quad \text{with } a_u \in \mathbb{N}. \tag{23}$$

Indeed, since it is clear that all $a_u \in \mathbb{N}$, we only need to show that w is lexicographically larger than every u occurring in the sum with nonzero coefficient a_u. Let $w_{\mathrm{red}} = (r_1, \ldots, r_k)$. By the very definition of the variable length shuffle product the first digit u_1 of any word u occurring in sum (23) has the form (possibly after rearranging terms)

$$u_1 = 0 + \cdots + 0 + r_1 + \cdots + r_1,$$

where the number N_0 of zeros and the number of terms r_1, say N_r, satisfy $N_0+N_r=a$. Moreover all possible values $0\leq N_0<a$ may occur in this way. Then it is clear that for the maximal lexicographic term m in (23) we have $N_0=0$, $N_r=a$ and the first digit m_1 of m must be equal to $a\cdot r_1=w_1$ (product in $\mathbb{N}$) where w_1 is the first digit of w. Notice that by definition of the variable length shuffle product we may use for the computation of the second digit m_2 of m only zeros or the second digit r_2 of r. The problem is thus reduced to the case $(w_{\mathrm{red}})\hat{}$ of length $\lambda(w)-1$. Thus induction with respect to the length of words proves (23). Consider now formula (23) for $w=l$, a Lyndon word with $a:=\gcd(l)>1$: the right side is homogeneous and l is the maximal lexicographic term. Thus by Corollary 3.3, if we write each $a_u u$ as a polynomial (over $\mathbb{Q}$) in the set of Lyndon words $\mathscr{L}$, the indeterminate l does not occur in any term $a_u u$ with $u<l$. Since l_{red} is a modified Lyndon word if l is a Lyndon word, this shows, replacing l by the homogeneous expression

$$l=(l_{\mathrm{red}})^{\uplus a}-\sum_{u<l}a_u u,$$

that we have

$$\mathbb{Q}[(\mathscr{L}\setminus\{l\})\cup\{l_{\mathrm{red}}\}]=\mathbb{Q}[\mathscr{L}].$$

This gives the possibility to replace every Lyndon l word by the corresponding Lyndon word. By [11, Theorem 6.1], the Lyndon words are algebraically independent polynomial generators for $\mathsf{QSym}_{\mathbb{Q}}$ and (13) shows that in every weight there are as many Lyndon words as there are modified Lyndon words. This guarantees that the set $\mathscr{L}^{\mathrm{mod}}$ of modified Lyndon words is algebraically independent over $\mathbb{Q}$ and the lemma is proven. □

Step 3. We already know by Lemma 3.4 that every word is a unique polynomial in the modified Lyndon words with coefficients in $\mathbb{Q}$. The only point is to show that these coefficients are all in $\mathbb{Z}$. To see this we write the words of weight N in canonical order on a list L_N. In the lowest weight we have $L_1=\{(1)\}\subset\mathscr{L}^{\mathrm{mod}}$ and $L_2=\{(2),(1,1)\}$. Now,

$$(2)=(1)^{\uplus 2}-2(1,1).$$

We can interprete this relation as

$$(2)=(1)^2-2(1,1)\in(\mathbb{Z}[\mathscr{L}^{\mathrm{mod}}],\uplus=\cdot) \tag{24}$$

where "$\uplus=\cdot$" indicates that the multiplication in $\mathbb{Z}[\mathscr{L}^{\mathrm{mod}}]$ is performed by writing elements as polynomials in the modified Lyndon words. Thus, assume that for some N and some word w of weight N the hypothesis $H_{N,w}$ consisting of the two parts:

$H_{N,w,1}$ All words having weight $<N$ belong to $(\mathbb{Z}[\mathscr{L}^{\mathrm{mod}}],\uplus=\cdot)$.

Let $\mathscr{M}_w$ be the $\mathbb{Z}$-module with basis all words u of weight N such that $u\succ w$.

$H_{N,w,2}$ For each word v of weight N preceding w in the canonical order there exists a unique monomial P_v in $(\mathbb{Z}[\mathscr{L}^{\mathrm{mod}}], \uplus = \cdot)$ such that

$$v - P_v \in \mathscr{M}_v, \tag{25}$$

Thus, v can be written as a unique monomial P_v in the modified Lyndon words modulo a unique linear combination lc_v of words that are canonically larger than v. Accordingly, we have

$$v = P_v + lc_v.$$

For $N=2$, formula (24) gives $P_{(2)} = (1)^2$ and $lc_{(2)} = 2(1,1)$. Since $(1,1) \in \mathscr{L}^{\mathrm{mod}}$ we see that $H_{2,w}$ is true for all words of weight 2. Next, assume $H_{N,w}$ to be true for some $N \geq 2$ and all words w of weight $N-1$. The first word in canonical order on the list L_N is the composition (N) of length 1. This element is symmetric and applying Corollary 1.6(a) we find that $(N) = (1)^{\uplus N} + lc_{(N)}$, where $lc_{(N)}$ is a linear combination of words having weight N and length at least 2. Furthermore, it has coefficients in $\mathbb{Z}$. We thus may assume $H_{N,w,2}$ for the word $w = (N)$. Let $H_{N,v,2}$ be true for some word v of weight N and consider the next word w in the canonical order. Write w as the maximal canonical term in the form (21). If $k > 1$, then it is clear that all $u \prec w$, intervening in this Eq. (21) are in $(\mathbb{Z}[\mathscr{L}^{\mathrm{mod}}], \uplus = \cdot)$ and the result follows. It remains case $k = 1$. Then $w = l^e$ for some Lyndon word l. If already $l^e \in \mathscr{L}^{\mathrm{mod}}$, then again we have the result. If not, the reason can only be the fact that $a := \gcd(l) > 1$. Then we have the homogeneous expression

$$(l_{\mathrm{red}})^{\uplus a} = l + \sum_{u \succ l} \gamma_u u \quad \text{with } \gamma_u \in \mathbb{N}.$$

Indeed the minimal canonical term in the expansion of this $\uplus$-power of l_{red} must have length $\lambda(l_{\mathrm{red}})$ and then it can only be l itself. Moreover this equation can be written as

$$l - (l_{\mathrm{red}})^{\uplus a} = -\sum_{u \succ l} \gamma_u u \in \mathscr{M}_l.$$

This means that we conducted the induction one step further. This process ends at $v = (1)^N$, the N-fold concatenation of the composition (1) and $(1)^N$ is a symmetric modified Lyndon word. Thus $H_{N,w}$ is seen to be true for all words w of weight N. This completes by induction the proof of the main theorem. □

We computed all words w of weight $|w| \leq 8$ in $\mathbb{N}_+^\star$ as polynomials of the modified Lyndon words and found perfect agreement with the theorem that all coefficients are rational integers in $\mathbb{Z}$. A list is available, [4].

We give a short list of elements in $\mathscr{L}^{\mathrm{mod}}$.

weight 1 (1).

weight 2 (1,1).
weight 3 (1,1,1), (1,2).
weight 4 (1,1,1,1), (1,3), (1,1,2).

Some expressions in $\mathbb{Z}[\mathscr{L}^{\mathrm{mod}}]$.

weight 2 $(2) = (1)^2 - 2(1,1)$.
weight 3 $(3) = (1)^3 - 3(1)(1,1) + 3(1,1,1)$.
$(2,1) = (1)(1,1) - 3(1,1,1) - (1,2)$.
weight 4 $(4) = (1)^4 - 4(1,1)(1)^2 + 2(1,1)^2 - 4(1,1,1,1) + 4(1)(1,1,1)$.
$(3,1) = (1,1)(1)^2 - (1)(1,1,1) - 2(1,1)^2 + 4(1,1,1,1) - (1,3)$.
$(2,2) = (1,1)^2 - 2(1)(1,1,1) + 2(1,1,1,1)$.
$(2,1,1) = -(1)(1,1,1) - 2(1,1,1,1) + (1,1,2) - (1,2)(1) + (1,3) + (1,1)^2$.
$(1,2,1) = (1,2)(1) - (1,3) - (1,1)^2 + 2(1)(1,1,1) - 2(1,1,1,1) - 2(1,1,2)$.

Acknowledgements

The authors are grateful to Jan Stienstra, Christian Kassel and Michiel Hazewinkel for helpful and stimulating discussions. They acknowledge their indebtedness to the referee who urged them by pertinent remarks to make the exposition more transparent.

References

[1] J.A. Dieudonné, Introduction to the Theory of Formal Groups, Dekker, New York, 1973.
[2] E.J. Ditters, Curves and formal (co)groups, Inventiones Math. 17 (1972) 1–20.
[3] E.J. Ditters, Sur une extension non-cocommutative d'algèbre de Hopf des fonctions symétriques, Rapport, Vrije Universiteit Amsterdam, 1985.
[4] E.J. Ditters, Note on free polynomial generators for the Hopf algebra of quasisymmetric functions together with a list of words of weight ≤ 8, Rapport, Vrije Universiteit, Amsterdam, 1998.
[5] I.M. Gelfand, D. Krob, A. Lascoux, B. Leclerc, V. Retakh, J.-Y. Thibon, Noncommutative symmetric functions, Adv. Math. 112 (1995) 218–348.
[6] M.E. Hoffman, The algebra of multiple harmonic series, J. Algebra 194 (1997) 477–495.
[7] I.G. MacDonald, Symmetric Functions and Hall Polynomials, Clarendon Press, Oxford, 1979.
[8] C. Malvenuto, C. Reutenauer, Duality between quasi-symmetric functions and the Solomon descent algebra, J. Algebra 177 (1995) 967–982.
[9] K. Newman, Constructing sequences of divided powers, Proc. Am. Math. Soc. 31 (1972) 32–38.
[10] D.E. Radford, A natural ring basis for the shuffle algebra and an application to group schemes, J. Algebra 58 (1979) 432–454.
[11] Chr. Reutenauer, Free Lie Algebras, Clarendom Press, Oxford, 1993.
[12] A. Scholtens, S-typical curves in non-commutative Hopf algebras, Thesis, Vrije Universiteit, Amsterdam, 1996.